DETAILED ACTION

Response to Amendment

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Frank R. Agovino (Reg. # 27,416) on 08/24/2009.

----------Begin Examiners Amendment----------

Claims 1-14 (canceled).

Claim 15 (currently amended): A method for providing a first service and a second service to a user via a client being coupled to a data communication network, said first service being provided by a first network server also being coupled to the data communication network, said second service being provided by a second network server also being coupled to the data communication network, said method comprising:

receiving a first request from the first network server to provide the first service to the user wherein the first service requires authentication of the user;

authenticating the user for the first service in response to the received first request;

allowing the user access to the first service in response to the received first request wherein an authentication ticket and profile information associated with the user is communicated to the first service;

storing first data on the client in response to allowing the user access to the first service, said first data identifying a first policy group associated with the first service, said first policy group having a shared set of business rules to restrict authentication of a user across different domains;

receiving a second request from the second network server to provide the second service to the user wherein authentication of the user by the second

service is optional and wherein the user is not authenticated for the second service;

if the second service is associated with the first policy group identified by the stored first data, allowing the user access to the second service in response to the received second request wherein the user is authenticated for the second service in response to the received second request and wherein the authentication ticket and profile information associated with the user is communicated to the second service; ~~and~~

if the second service is not associated with the first policy group identified by the stored first data:

updating the stored first data to identify the second service, said updating further comprising identifying a second policy group associated with the second service; and

allowing the unauthenticated user to access the second service during which the user continues to be unauthenticated for the second service wherein authentication ticket and profile information associated with the user is not communicated to the second service;

receiving a third request from a third network server to provide a third service to the user, said third network server also being coupled to the data communication network;

authenticating the user for access to the third service in response to the received third request; and

allowing the user access to the third service if the user has been authenticated,

wherein, in response to allowing the user access to the third service, the user is allowed access to the second service on a subsequent visit to the second network server if the third service is associated with the second policy group identified by the updated first data.

Claims 16-29 (canceled).

Claim 30 (currently amended): A system for providing services to a user, said system comprising:

a first network server coupled to a data communication network, said first network server being configured to provide a first service to a user via a client also coupled to the data communication network, said first service requiring authentication of the user;

a second network server coupled to the data communication network, said second network server being configured to provide a second service to the user via the client, wherein the authentication of the user by said second service is optional;

a central server coupled to the data communication network, said central server being configured to receive a first request from the first network server to provide the first service to the user and a second request from the second network server to provide the second service to the user;

a database associated with the central server, said database configured to store a 64 bit PUID corresponding to the user to be authenticated, said database providing said 64 bit PUID to the central server to allow the central server to authenticate the user, said database being further configured to store information identifying a first policy group associated with the first service and a second policy group associated with the second service, wherein the first policy group defines a shared set of business rules to restrict authentication of a user across different domains and the second policy group defines a shared set of business rules to restrict authentication of a user across different domains;

wherein, in response to the received first request, the central server is configured to allow the user access to the first service and to generate and store first data on the client based on the stored information identifying the first policy group associated with the first service, said first data identifying the first policy group associated with the first service wherein the central server authenticates

the user for the first service in response to the received first request, wherein the user is allowed to use the first service for a predefined period of time;

wherein if the second policy group identified by the stored information identifying the second policy group associated with the second service is the same as the first policy group identified by the stored first data, the central server is configured to allow the user access to the second service in response to the received second request wherein the user is authenticated by the central server for the second service in response to the received second request; and

wherein if the second policy group identified by the stored information identifying the second policy group associated with the second service is not the same as the first policy group identified by the stored first data, the central server is configured to update the stored first data to identify the second service in response to the received second request and the central server is configured to allow the unauthenticated user to access the second service during which the user continues to be unauthenticated for the second service.

Claim 31 (canceled).

Claim 32 (previously presented): The system of claim 30, wherein the second network server is being configured to generate and store second data on the client if the second policy group identified by the stored information identifying the second policy group associated with the second service is not the same as the first policy group identified by the stored first data, said second data indicating that the second network server has communicated the second request to the central server, said second request indicating a desire of the second network server to provide the second service to the user; and

wherein on a subsequent visit to the second network server by the user, the second network server is configured not to direct a request to the central server to provide the second service to the user if the second data is stored on the client.

Claim 33 (original): The system of claim 30, wherein the updated first data further identifies the second policy group associated with the second service.

Claim 34 (previously presented): The system of claim 33, further comprising:

a third network server coupled to the data communication network, said third network server being configured to provide a third service to the user via the client;

said central server being further configured to receive a third request from the third network server to provide the third service to the user and to authenticate the user for access to the third service in response to the received third request;

wherein the stored information identifying the third policy group associated with the third service further identifies a third policy group associated with the third service, the third policy group defines a shared set of business rules to restrict authentication of a user across different domains; and

wherein the central server is configured to allow the user access to the second service on a subsequent visit to the second network server if the user has been authenticated and if the third policy group identified by the stored information identifying the third policy group associated with the third service is the same as the second policy group identified by the updated first data.

Claim 35 (currently amended): One or more computer-readable media having computer-executable components for providing a first service and a second service to a user via a client being coupled to a data communication network, said first service being provided by a first network server also being coupled to the data communication network, said second service being provided by a second network server also being coupled to the data communication network, said computer-readable media comprising:

a redirect component for receiving a first request from the first network server to provide the first service to the user and for receiving a second request from the second network server to provide the second service to the user, wherein the user is allowed to use the first service for a predefined period of time;

a response component for storing first data on the client in response to the received first request, said first data identifying the first service wherein authentication of the user by the first service is optional and wherein the user is not authenticated for the first service and not authenticated for the second service and wherein the user is allowed to access the first service without authenticating the user during which the user continues to be unauthenticated for the first service and unauthenticated for the second service;

an authentication component for allowing the user access to the second service in response to the received second request wherein the second service requires authentication of the user and the user is authenticated for the second service in response to the received second request;

a storage component for storing a 64 bit PUID corresponding to the user to be authenticated, said storage component providing said 64 bit PUID to the authentication component to allow the authentication component to authenticate the user, said storage component further storing information identifying a second policy group associated with the second service, wherein the stored first data further indicates a first policy group associated with the first service wherein the first and second policy groups are stored in a database coupled to a central server; and

wherein, in response to the authentication of the user by the second service, the authentication component is adapted to authenticate the user for the first service identified in the stored first data if the second policy group identified by the stored information in the storage component is the same as the first policy group indicated by the stored first data.

Claim 36 (canceled).

Claim 37 (original): The computer-readable media of claim 35, wherein the first request indicates a desire of the first network server to provide the first service to the user, wherein the response component is adapted to store second data on the client in response to the received first request, said second data indicating that the first network server has requested to provide the first service to the user, and wherein on a subsequent visit to the first network server by the user, the first network server is adapted not to request to provide the first service to the user if the second data is stored on the client.

Claim 38 (currently amended): The computer-readable media of claim 37~~, further comprising:~~

~~a storage component for storing information identifying a policy group associated with the second service;~~

~~wherein the stored first data indicates a policy group associated with the first service; and~~

wherein, in response to allowing the user access to the second service, if the second policy group identified by the stored information is the same as the first policy group indicated by the stored first data, the response component is adapted to render a web page to the client, said web page including an image tag directing to a script of the second service, said script adapted to delete the second data from the client.

Claims 39-40 (canceled).

----------End Examiners Amendment ----------

Status of the instant application:

- Claims 15, 30, 32, 33, 34, 35, 37 38 are pending in the instant application.

Response to Arguments

Applicants, examiners amendments filed 08/27/2009 have been fully considered and have been found to be persuasive, please see the office action below.

Allowable Subject Matter

2. Claim(s) 15, 30, 32, 33, 34, 35, 37, 38 are allowed, but renumbered as (1 - 8)

3. The following is an examiner's statement of reasons for allowance: applicant's amendment to the claims to effect the examiners amendment has been found to be persuasive.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANT B. SHAIFER HARRIMAN whose telephone number is (571)272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

09/09/2009

/Dant B Shaifer - Harriman /
Examiner, Art Unit 2434

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434